

## **Techno-economic evaluation of a cost-efficient standard container monitoring system**

Bart Lannoo, Bram Naudts, Erik Van Hauwaert, Peter Ruckebusch, Jeroen Hoebeke, Ingrid Moerman

*Department of Information Technology, Ghent University - IBBT, Gent, Belgium*

[bart.lannoo@intec.ugent.be](mailto:bart.lannoo@intec.ugent.be)

# **Techno-economic evaluation of a cost-efficient standard container monitoring system**

The main goal of this paper is to give an overview of the container monitoring solution as proposed in the IBBT MoCo project, with a focus on the operational savings. A high-level architecture of the monitoring systems is presented and different power modes of the container gateway are introduced to ensure an increased energy efficiency of the battery powered container gateways or MoCo devices. Our operational cost model provides valuable insights in the relation between on the one side the chosen system architecture and power modes and on the other side the expected data connection costs and energy consumption. By using different power modes of the MoCo device and optimizing the design parameters, the battery lifetime can be increased to three years or more, which makes the MoCo solution a very robust monitoring system.

Keywords: techno-economic model; operational expenses; data connection costs; energy consumption; wireless sensor networks; container monitoring; container tracking

## **Introduction**

Container shipping is the most commonly used mode of transport for international cargo trading. The global container system faces important challenges including increased security requirements and a demand for more efficient and cost-effective transportation services. The US Container Security Initiative, for example, requires products to be traced during transport and demands a full trace to be delivered 24 hours before arrival. A 2009 study carried out by IBM among hundreds of Supply Chain Officers in multinational companies showed that supply chain visibility (i.e. traceability of products) is seen as the single most important challenge impacting supply chains (before risk and cost management), requiring versatile ICT platforms. The above requirements comprise of container intrusion detection, container tracking and cargo monitoring. State of the art industrial monitoring systems live up to the necessary

security requirements, but do not manage to balance this with the demanded cost-effectiveness. The IBBT project MoCo (Monitoring of Containers) proposes a cost-efficient smart monitoring system to overcome the above shortcomings.

The main goal of this paper is to give an overview of the MoCo solution with a focus on the operational savings. The proposed system is capable of monitoring the container's position, door seal and cargo. This monitored info is communicated to the wayside via a wireless data network without incurring high operational costs. Given that stacked containers are a very hostile environment for wireless data communication, a robust communication system must be in place to ensure that containers can communicate with the outside world. The container gateway is using different power modes throughout the container handling, to ensure increased energy efficiency of the battery powered container gateways and cargo sensors.

Starting from message frequency, network availability, message size and power consumption an analytic techno-economic model forecasting operational costs has been developed, which is then applied to different scenarios to assess the cost-effectiveness and sensitivity of the proposed system. Our operational cost model provides valuable insights in the relation between on the one side the chosen system architecture, communication hierarchy and power modes and on the other side the expected data connection costs and energy consumption. Different scenarios are evaluated to show the impact of the used power mode, the message frequency, the number of cargo sensors, the battery type, etc. We believe that the proposed monitoring system can achieve the required balance between the security goals driven by the customs and government and the demanded cost-effectiveness from the logistics sector.

In section 2, an overview is given of technologies and solutions currently available on the market, with a view on their shortcomings. Section 3 describes the

technical solution of the MoCo system via a high-level system architecture which makes use of the advantages in flexibility and cost of wireless sensor networks (WSNs). In section 4, the economic environment in which the system would operate is described via a value network consisting of business roles with actors and their interactions. These serve as input for a techno-economic analysis of the operational costs in section 5. Finally, in section 6 the main conclusions are given.

### **Related work**

Several endeavours in the field of container monitoring have been done. Most of the systems that are used today for monitoring containers use RFID (Radio-frequency identification) tags to monitor the goods inside the container or to monitor the container itself. The range of these RFID tags is very limited and it is not possible to access this information over a longer distance.

Only recently, researchers have started to use wireless sensor networks (WSNs) for monitoring containers. Mahlke describes an architecture of low power WSNs for container tracking and monitoring applications [1]. The system architecture uses three devices. First, an internal monitor with sensor nodes, second a container monitor with a WSN interface, GSM (Global System for Mobile Communications) and GPS (Global Positioning System) and last a prime monitor which functions as an infrastructure node. The topology selection is dependent on the kind of communication. Inter container communication is organized in a star or mesh topology and intra container communication can be organized with a chain like topology for trains or a mesh topology for ships. Schaefer proposes a safe and secure solution for monitoring containers [2]. For wide range communication, GSM/GPRS or satellites are used; short range communication inside the container is provided by ZigBee. Each container needs to be equipped with a device that either has a GSM or satellite receiver, making the

device cost expensive. Networking between the containers is not considered. A meshed Bluetooth network is established if one or more containers do not have a working satellite uplink. The MASC (Monitoring and Security of Containers) system, as described by Lauf, introduces a similar container monitoring system that collects data from sensors inside the container [3]. These sensors are wired connected to an outside antenna that directly reports to a base station. No mesh networking between the containers is used. The communication between the container and the remote server is push-based, because the MASC units are battery powered. All of the solutions above do not fully investigate the communication issues, but mainly focus on providing services. The communication part is handled by standardized components, i.e. ZigBee or Bluetooth, and mostly focuses on direct communication between a container and an external network, and without cost and power consumption optimizations.

Tests performed by Rogoz showed that communication between containers experiences problems due to multipath propagation [4]. They propose to use multihop routing in order to cope with these problems. A test with sensor nodes running the ZigBee standard showed that communication is only possible between adjacent containers. No multi hop solutions were proposed. In [5], Rogoz developed a single hop solution that is able to track containers in a stacked container environment using wireless sensor nodes. The tracking is done by a sensor node gateway, attached to a PDA (Personal Digital Assistant). The proposed solution is similar to a subset of the MoCo device – MoCo reader interaction proposed in this paper (see next section) and only focuses on this specific functionality. The Intelligent container project described by Jedermann [6] and Lang [7] uses a combination of RFID and sensor nodes within one container. The sensor nodes are battery powered and use 802.15.4 to communicate with a gateway. The gateway communicates with the wayside using different mobile

networks, such as WLAN (Wireless Local Area Network), GPRS (General Packet Radio Service), or UMTS (Universal Mobile Telecommunications System), depending on availability. The goal is to monitor quality changes that could occur during transport and to reduce the data exchanged. This is done by sending already processed data instead of raw sensor measurements. The gateways are powered with the same power supply as the cooling aggregate. This implies that the technology can only be used on reefer containers. Communication between containers was not considered. Kim proposes a hierarchical architecture with on the one hand an internal container network for communication using a combination of RFID tags and sensor nodes; and on the other an external network between containers that uses more powerful gateways, using an IEEE 802.11 interface or a GPRS modem [8], [9]. In this architecture, each container needs to be equipped with such a gateway, making it cost expensive. This research group is also the first one who has conducted a real-life experiment in a 3x3 stacked container configuration. They found that energy consumption is critical, which is in line with our findings. Yeoh discusses the basic requirements that are needed to form an autonomous cargo monitoring system with WSN and proposes a containerized cargo monitoring system based on WSNs [10]. Tilt/motion sensors are incorporated to improve the network convergence time of container networks and further network nodes are periodically switched into sleeping mode to save energy and extend the lifetime of the network. The solution is also technically implemented on a real container vessel. Some important concepts of this solution are in line with the container monitoring system proposed in the MoCo project. However, the different power modes of the container gateway will further optimize the power consumption of the MoCo solution.

Next to the technical solution, the economic feasibility and used business model is another important aspect which is tackled in the MoCo project. In the above related

work, the economic aspects are only considered by Schaefer [2]. In this solution, the shipper of containerized goods is paying for improved supply chain visibility, and therefore owns the collected data for their respective shipments. The owner of data can define who they share the data with and under what conditions. The data can be combined with other shipment related data from RFID readers, supply chain or warehouse management systems, import/export declaration systems, and more. A single central database containing data concerning and provided by many parties is from a data privacy perspective out of the question.

### **Proposed solution for monitoring containers**

In this paper we describe the MoCo monitoring system that makes use of a sensor network to monitor the door seal, the position and (optionally) the cargo of a container. The data is communicated to the wayside via a wireless data network. This solution is optimized to have a low operational cost by reducing message frequency and power consumption through a dedicated communication protocol. First the high-level architecture of the MoCo system is given, and in a second subsection the different communications technologies and the radio state power modes are presented.

#### ***High-level architecture of the container monitoring system***

Figure 1 shows a high-level overview of the container monitoring architecture with its different components and connections, as defined within the MoCo project. The MoCo solution consists of ad-hoc, self-organizing and dynamic container networks using intra-container communication (inside a container from the cargo sensors to the container gateway or MoCo device), inter-container communication (between the gateways or MoCo devices of two or more stacked containers) and extra-container communication (between the container gateways or MoCo devices and an external network). These

three hierarchical types of communication ensure the robustness of the communication between the container and the wayside. Monitoring the door seal, by using an integrated door sensor, is a main requirement, but optional sensors can be added to the container's wireless sensor network (WSN) to enrich the product offering with extra functionality such as the detection of intrusion through other surfaces of the container, temperature and humidity measurements, shock and vibration monitoring, etc.

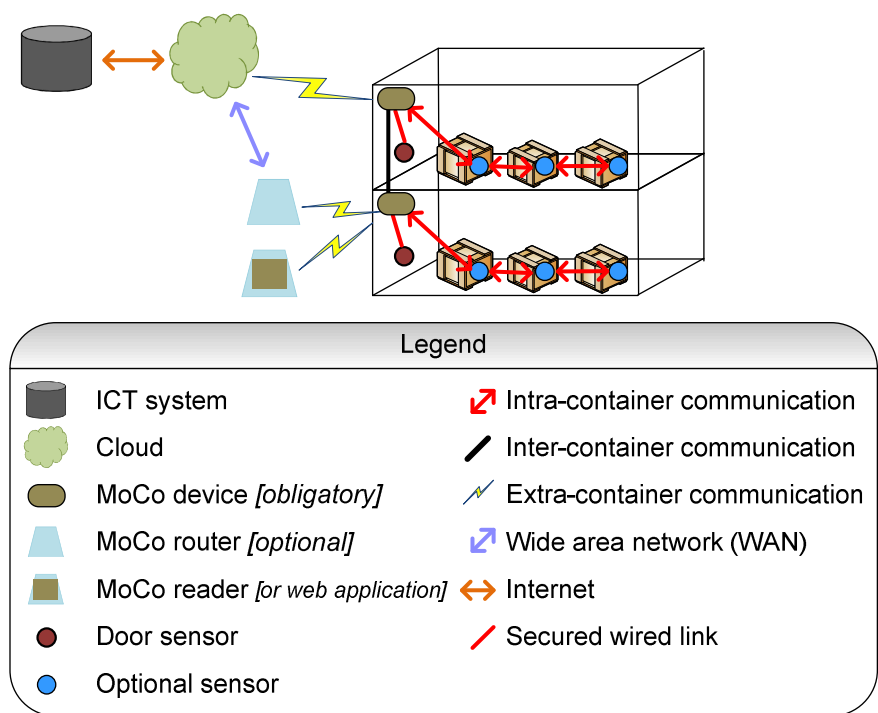


Figure 1. High-level architecture of the container monitoring architecture

Next to the MoCo device, the MoCo router and the MoCo reader are two other specific components in the MoCo architecture. In order to reduce the energy consumption and roaming costs of a MoCo device, MoCo routers will be installed on logistic sites (i.e. terminals/quays) to bundle the communication radiated by the different MoCo devices within reach. MoCo readers are used to confirm/disconfirm sealing/unsealing of the door, and to read information stored on the MoCo device and/or in the cloud for a container within its reach.



### *Communication technologies and radio state power modes*

It is a key requirement that the communication from the MoCo devices to the outside world must be as energy-efficient and low-cost as possible. For that reason, 802.15.4 technology is chosen where possible, and is always preferred over the considered wide area network technologies GSM/UMTS. 802.15.4 technology is used for intra- and inter-container communication, and for extra-container communication between the MoCo device and MoCo router, while GSM/UMTS communication is used for extra-container communication from the MoCo device directly to the cloud. It is clear that the MoCo router is preferred as gateway to the outside world, since it can be reached by a MoCo device over the lower-power 802.15.4 network and the MoCo router will typically incur no roaming costs as it will be directly connected to the Internet.

The radio state diagram in Figure 2 illustrates for the MoCo device three different power modes that are used throughout container handling to ensure increased energy efficiency of the battery powered MoCo devices.

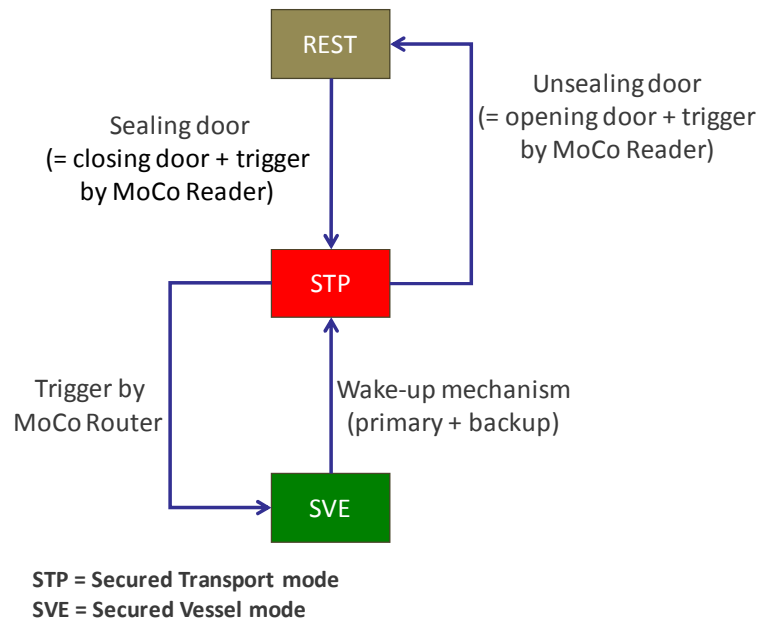


Figure 2. MoCo device radio state modes

When the container is stored (and not stuffed), the MoCo device will be in REST mode. In this mode, the MoCo device will monitor and transmit its position (using its GPS) and battery level on a daily (default) or x-daily (configurable by the MoCo reader or cloud) basis to the cloud. Next to this, the door sensor will monitor any opening/closing of the container doors. The 802.15.4 radio is active, but operates using a highly energy efficient sleep schedule (iterating sleep and wake-up periods).

If the container is stuffed, the MoCo device will be put in secured transport (STP) mode. The door sensor detects that the doors of the container are closed and in addition a MoCo reader will send a trigger to the MoCo device to indicate that the doors have been sealed and that the container will be shipped. In STP mode, 2-hourly (default) or x times 2-hourly (configurable by MoCo reader or cloud) transmission of the position, battery level and the reports of the optional sensors will take place. In addition to these 2-hourly or x times 2-hourly transmissions, immediate transmissions upon door opening, safety violations or critical events will take place.

Once the container is loaded in the vessel, the MoCo device can be switched to a highly energy efficient mode, called secured vessel (SVE) mode. In order to be able to inform a MoCo device that the container is to be loaded in the vessel, an external trigger is needed. Since the GSM/UMTS radio will sleep most of the time, it is preferred that this trigger comes from an 802.15.4 capable device, i.e. the MoCo router. The MoCo router informs the MoCo device about the loading of the container in the vessel, the link with the vessel and optionally the loading/unloading plan of the vessel. The MoCo device now remains in SVE mode during its transport in the vessel.

### **Techno-economic model**

The technical solution to monitor containers, as developed within the MoCo project, offers potential value to several companies that are involved in the transportation of

containers. To maximize this value, both for the client and for the MoCo consortium, the product offer must fit within a value network of many companies that are all willing to cooperate. In this section, we first present the different involved actors and the MoCo product offer. Afterwards, we identify the main operational costs associated with the MoCo system. It will be very important to keep these operational costs under control and in balance with the service revenues to build a positive business case for the different actors involved.

### ***MoCo product offer***

The way the MoCo monitoring system is offered and sold to potential customers can be implemented in different manners. Since continuous revenues from service offering are often a more sustainable business than purely manufacturing, the MoCo business model will be based on offering different services in its product offer. In this subsection, we describe the services and products that are offered to the customers and other stakeholders (e.g. customs, society, ...) to realize added value for them.

### ***MoCo services***

*Certificates.* The main goal of the MoCo system is to offer reliable and transparent container transport. This results in two certificates that can be bought:

- **Security Certificate:** the MoCo device monitors the door status and reports if and when the container has been opened. If no positive report was received, the container is certified not to have been opened without proper authorisation. This can speed up customs' operations.

- **Condition Certificate:** the MoCo device monitors not only the door status, but also all optional sensors that are present in the container. Regular updates and a complete log of the container and its payload are available this way.

The certificates require that the container is fitted with a MoCo devices connected to relevant ICT and, when applicable, that optional MoCo-certified sensors are bought and installed as well.

*Data traffic.* A container which has been fitted with a MoCo device will frequently communicate with the cloud. If a Certificate has been sold, the costly communication over a mobile network is taken care of. However, when no certificate has been sold, the device may still communicate with the cloud (though less frequently). This can be useful for the container provider, e.g. for localization purposes. To cover these costs, the MoCo consortium offers a data traffic subscription to allow the devices to transmit information in the absence of a certificate and it is required for the MoCo device to be used. This cost can be avoided by the customers of the MoCo consortium, however, both by making sure a Certificate is sold for most of the time, and by placing the container close to a connected MoCo router for the remainder of the time.

*Announcement to warehouse management system (WMS).* By equipping containers with a MoCo device, they can be traced and monitored. This information can be passed on to interested parties' data warehouse. An interesting customer appears to be the terminal, as they can use this to keep track of the container flow (in and out). A small amount is charged for each MoCo container that passes through a terminal, in return for supplying the terminal this information.

*Specific applications.* Specific applications can be developed (and will probably be offered through the Service Platform). An example would be aggregated data and data analyses of containers, their movements and contents. Such a report can be purchased (provided that the data does not contain sensitive information, of course).

#### *MoCo hardware*

In order to provide the above services, the hardware provided by the consortium will be either produced or required. This includes the MoCo devices, routers, readers and optional sensors. The pricing of this hardware will depend on the device type, functionality, volume etc.

#### *MoCo Service Platform access*

The MoCo system offers much information within the cloud. A Service Platform will be available to get all requested information of a container, as well as configuration and management options. A subscription fee is required to get access to this service platform.

#### *Actors and their interactions*

The economic environment in which the system would operate is described via a value network consisting of business roles with actors and their interactions. A high-level categorization of the actors that are involved in a container handling process and that will benefit from a container monitoring system, are presented in this section. Actors are entities in a value chain that can perform one or multiple business roles. Due to the roles they have taken, actors will interact with each other and the value network determines the operational and economic relations between them. These interactions involve the delivery of information, products or services. The efforts of the actors are compensated

by payments and in this way, the value network can be used to identify the cash flows within the project. Note, however, that quantifying the cash flows requires both a detailed insight into the costs incurred by the actor and assumptions on the tariff schemes used. We describe the different actors with their different business roles.

### *MoCo Consortium*

The business management division determines the commercial and technological strategy. It is responsible for networking and building partnerships. Additionally, it manages the ICT aspects of the company, as well as the Intellectual Property Rights. Finally, it is responsible for selling the product offer to clients, carrying the connection cost of the devices and managing all involved hardware (e.g. firmware management, device configuration, handling own routers on clients' property, etc). The hardware division develops and sells the hardware (MoCo devices, MoCo routers, MoCo readers). It also develops firmware for the hardware and maintains this through the life cycle of the product (version management). The cloud operator division develops, maintains and provides access to the Service Platform, which it can either develop and maintain itself, or out-source to a third party.

### *Shipping Line*

The shipping line handles containers on the docks. Sometimes they own the containers, other times they rent them. Here, we do not distinguish between these cases and consider the shipping line to work closely together with the container provider in case it is a different company. From this point of view, a first role is to buy, install and maintain the MoCo devices. The shipping line also needs to update its ICT system in order to develop and maintain an interface with the Service Platform, as well as provide a CRM interface to its customers to make use of the new functionalities offered by the

MoCo solution. The shipping line will use the Service Platform to collect data. This information can be used to increase efficiency of its operations (e.g. for customs), but it can also sell data (bundled in certificate) to its customers. Finally, the shipping line will have to adapt its operations related to the MoCo containers, as they may have to receive special attention (e.g. checking up on battery power, placing containers close to the MoCo router, ...). Minimizing this operational cost is one of the goals in the MoCo product design.

### *Shipper*

The shipper needs to adapt its operations to distinguish MoCo equipped containers from regular containers. This includes sealing the container using the MoCo device according to customs' requirements. If the product company has requested it, optional MoCo sensors can be added during stowing of the container. In order to provide and receive all relevant data, its ICT system will have to be adapted to gain access to the Service Platform. The shipper should also provide data to the Service Platform to enable specific applications.

*Destination Co.* The destination company provides the shipper with detailed shipping instructions. This will help the shipper to decide which Certificate to purchase and which optional MoCo sensors to use.

### *Terminal Owner*

The MoCo routers are installed at the terminal as part of a package deal. They are connected to the available backhauling link and WMS. The terminal owner can adapt its ICT system to connect with the Service Platform in order to receive notice when containers enter or leave the terminal.

## Customs

Customs should accept the usage of the MoCo solution as a control mechanism and acquire MoCo readers or other means to access the web application for (un)sealing containers. This application will allow customs to check and pass containers. Note that it is expected that customs will not be willing to pay for anything. A cost sharing initiative could be launched with the other actors, where they jointly carry the cost of equipping customs.

## Cash flows and interactions between the different actors

The actors will interact by playing their roles. Usually there will be a cash flow involved in this interaction. Figure 3 indicates the external cash flows that can be identified from the roles appointed to each actor. Note that we call the sale of functionalities of the MoCo solution “Certificates” for all actors. This does not necessarily imply that the certificates are simply sold in the exact same form from one actor to the next. The Certificates in their pure form are sold to the Shipping Line, which can decide independently how it will sell the resulting functionalities to its customers and at what price.

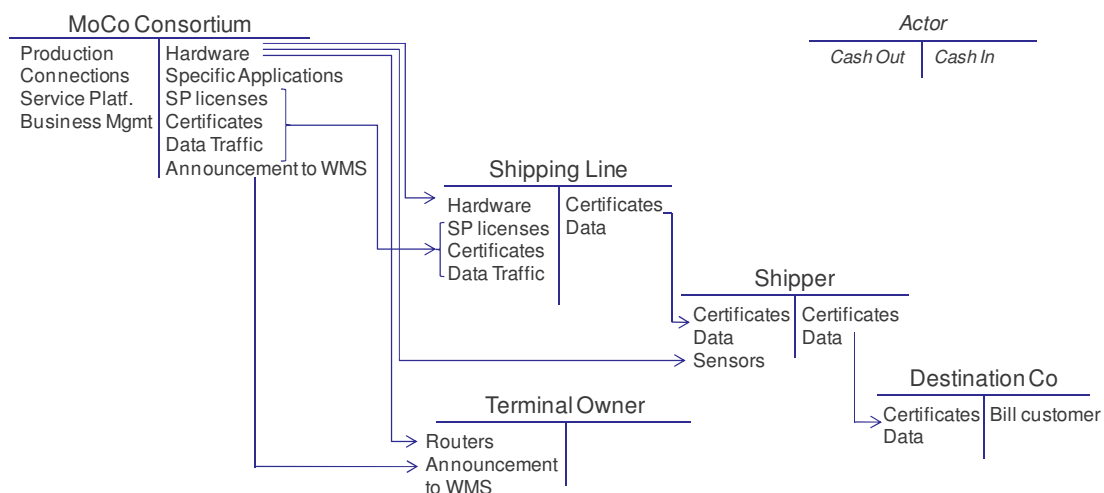


Figure 3. Cash flows from interactions between actors



### *Operational cost model*

Most of the container handling processes are identical to the current situation and the only impact is that the MoCo device needs to communicate to the ICT systems of the different involved actors. The changes in the processes for the shipping line and other involved actors are deliberately limited and will not outweigh the advantages of having the additional information of containers through the MoCo system. Therefore, we only look at the two (three) costs that do have an important impact on all partners involved: mobile roaming costs of communication, power consumption costs of the MoCo devices (and the battery replacement process). Note that there is an important difference between those costs: the mobile roaming costs are carried by the MoCo consortium and then distributed (with a profit margin) to the customers. The power consumption cost is to be carried by the customers – but it is in the consortium’s best interest to minimize operational costs for optimal customer satisfaction, because the sector is very sensitive on this point (e.g. avoiding additional overhead costs for battery replacements). Another important operational cost which is not evaluated in this paper, is the cost related to operating the management platform.

The operational cost models for mobile roaming and power consumption are based on the actual use of the MoCo device. These costs will indeed depend on the number and type of connections made. Therefore, there is a common part to both cost models, and they are using following input parameters:

- The number of weeks in each power mode (STP, SVE, REST)
- The connection frequency in each mode
- Message size, assumed to be 150 bytes

### *Mobile roaming*

Apart from the general input, there is additional input required for the mobile cost calculation, namely the data tariffs. Through contacts with network operators, a cost indication was obtained. There will be a general subscription cost per month and per active SIM card. On top of that there is a surplus based on the amount of traffic included in the subscription, with a minimum granularity of 1 MB. Traffic outside of the bundle is significantly more expensive, and therefore the subscription should be chosen such that it is very rare to require more data than what is included.

Based on the general input parameters, we can calculate the amount of time spent in each mode. Given the message frequency in each mode, this gives us an estimate of the amount of messages sent. Multiplying this by the message size leads to the total data usage over a period of time. The most intensive connection mode is STP. In the expected configuration (2-hourly messages), a full month of operating in STP mode only causes a traffic amount which is well under the lowest bundle of 1 MB per month.

### *Power consumption*

For the power consumption model, the basic principle is the same. First, the power consumption rates were investigated, and the used figures are based on the specification documents from manufacturers. These state the input voltage of the main components of the MoCo device (UMTS controller, GPS controller, ZigBee controller, MicroController) as well as their current draw in active and passive mode. Based on the modes and message frequency, the total consumed power can be calculated. Again, STP is by far the most power-intensive mode. Power will be provided by batteries, and we have compared three battery types in the model, as shown in Table 1.

Table 1. Batteries compared in the model

<b>Battery type</b>	<b>Power rating (kAs)</b>	<b>Price (EUR)</b>
Lithium AA	8.8	9.79
Lithium D	68.4	19.95
Lithium DD	126	66

Lithium D batteries are cheapest in terms of components, delivering the most power per EUR. However, Lithium DD batteries have more power and therefore last longer – requiring less battery replacement procedures. On the other hand, it is theoretically possible to use more than one battery in parallel (this delivers the same voltage to the attached components, and spreads power usage over all batteries).

### *Scenario analysis*

The operational cost model is applied to different scenarios with a varying number of weeks per power mode and a variable connection frequency. We start from a base case scenario and then we perform a detailed scenario comparison to estimate the battery lifetime (based on the number of weeks per power mode and the connection frequency).

### *Base case*

As a reference case, we take the case where a container does three deep-sea trips of 6 weeks in a year. This means the container is about 17 weeks in SVE mode (container wakes up a little earlier), and we expect an additional 10 weeks in STP mode before and after shipping. The remaining 25 weeks in that year, the container is in REST mode. The configuration is such that the container sends an update every two hours in STP mode. In SVE mode, no messages are sent, but there is a connection check twice a day. In REST mode, there is a single status update every day. In this case, the model calculates that there is on average 130 kB of traffic per month, meaning that a data bundle of 1 MB per SIM card is sufficient for transferring the expected monitoring data.

There is also a current draw of nearly 9Ah (operating at 3.6V). Table 2 displays the cost and expected life-time of the different battery types, with a life time of ca. 3.3 years for Lithium DD batteries. In the remainder of this paper, Lithium DD batteries are assumed.

Table 2. Battery results

<b>Battery type</b>	<b>Battery cost (EUR/yr)</b>	<b>Life-time (yr)</b>
Lithium AA	42.8	0.23
Lithium D	11.3	1.77
Lithium DD	20.2	3.26

### *Scenario comparison*

The base case scenario gives an estimate of the order of magnitude of the costs, but it does not tell us how sensitive this is to changes in the input parameters. As these input parameters are still uncertain, it is useful to investigate the impact of changes in the most relevant input parameters.

In the base case scenario, we assumed that the device remained in REST mode for 25 weeks, in SVE mode for 17 weeks and the remaining 10 weeks in STP mode. Overall, the cost impact is rather limited if the operational replacement cost of the battery is not taken into account. However, note that in the case of 42 weeks in STP mode, the expected life-time of a Lithium DD battery drops from 3.3 years to 1.3 years. The most important factor is the number of weeks in STP mode, as the SVE and REST modes have similar and much lower power consumptions. Note that the mobile roaming costs remain the same as the 1 MB data limit is more than sufficient as long as security and communication protocols are optimised to limit data traffic (without losing functionality).

The message frequency is the second factor that can have a significant influence on power consumption. For simplicity reasons, we now simply look at the impact of the message frequency in STP mode, and only look at the power consumption impact. The

previous section showed that mobile roaming costs will not deviate by much and that SVE and REST mode are similar in terms of power consumption, so these simplifications do not have an important influence on the results. Figure 4 and Figure 5 display the results graphically. It is clear that mostly UMTS is very sensitive to the number of connections made in terms of power consumption.

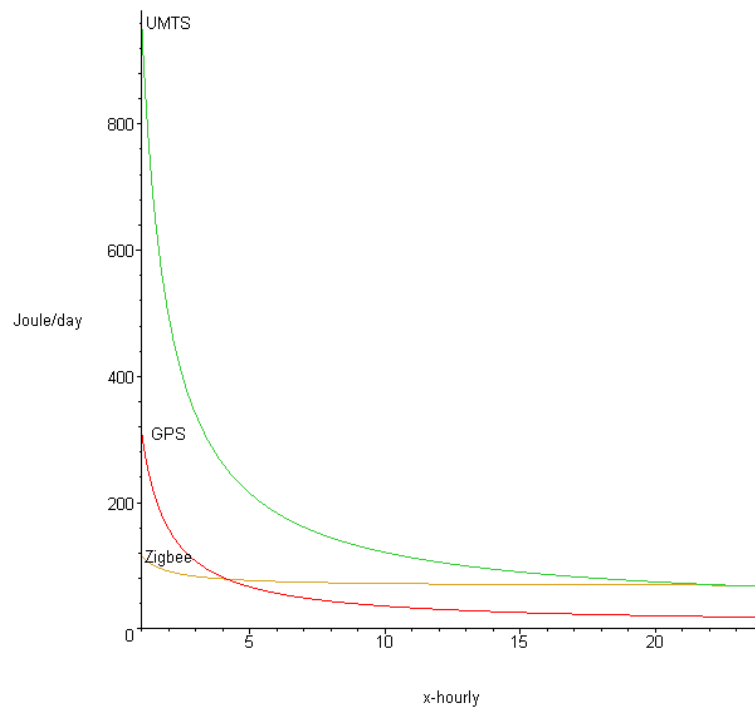


Figure 4. Impact of x-hourly message frequency for all technologies separately

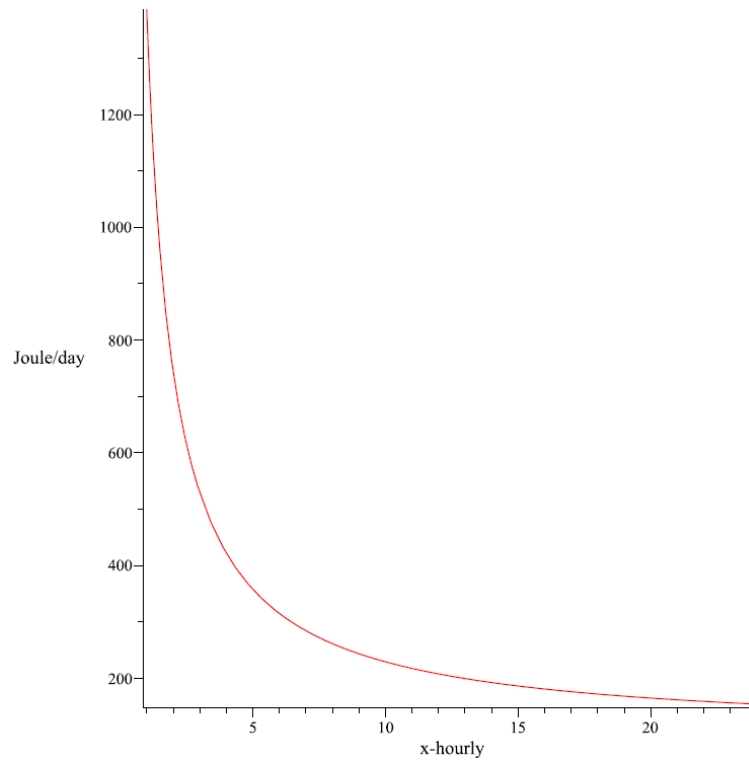


Figure 5. Impact of x-hourly message frequency for the device in its entirety

Combining all technologies in the device, a turning point seems to be at around a 4 to 6 hour message frequency. Passing that point increases the power consumption rapidly, while the power consumption remains rather stable below that point. We can display these results in a way that is more readily understandable: what is the life expectancy of the device in case of x-hourly message frequency for a device that is a certain number of weeks in STP mode (assuming that all other weeks of the year are REST mode, as REST and SVE are very similar in terms of power consumption). This is shown in Figure 6 and Figure 7.

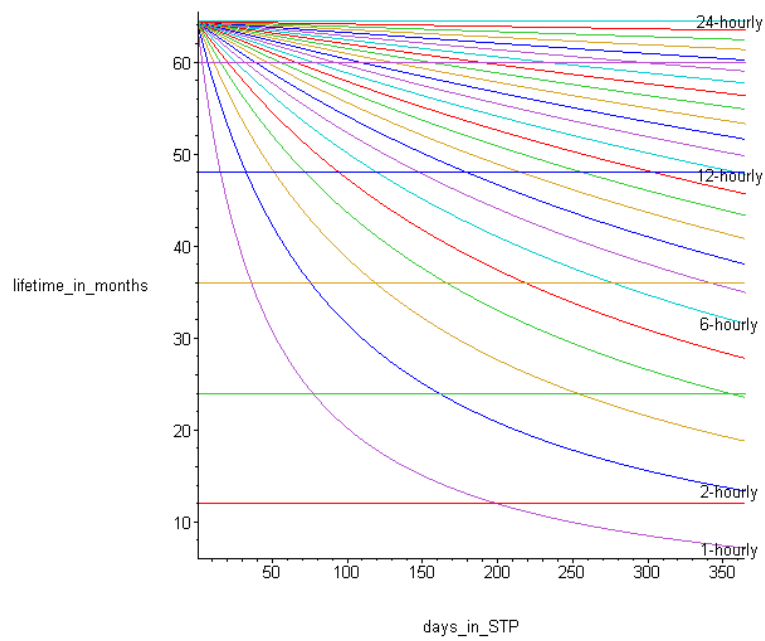


Figure 6. The expected life-time of a Lithium DD battery, given the number of days in STP per year and the message frequency

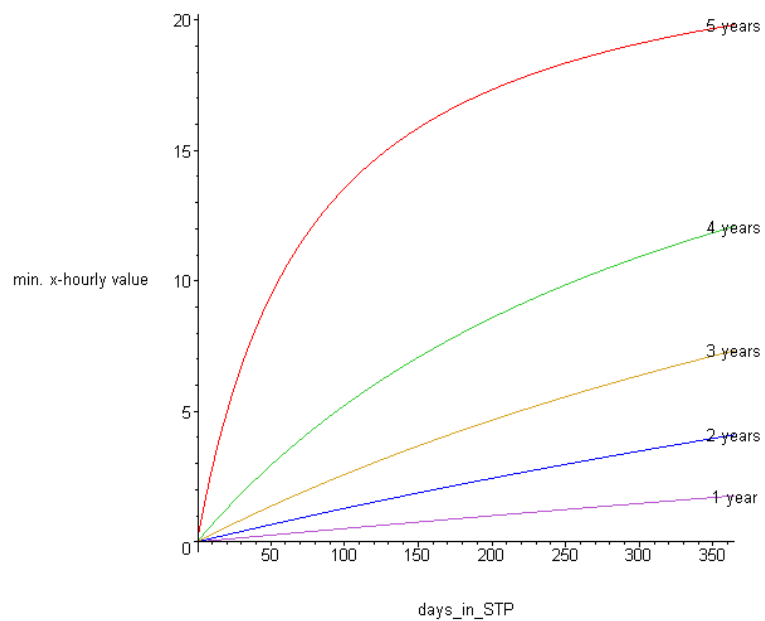


Figure 7. The message frequency allowed to reach an x-year life-time of a Lithium DD battery, given the number of days in STP mode

It is shown again that using a 4 to 6 hour interval, a battery life-time of about 2 to 4 years can be expected, depending on the number of days in STP mode. Using a 2 hour interval, as was assumed initially, shows a life-time of about a year in the most extreme cases. It is thus of utmost importance to design the container monitoring system in a proper way to achieve a feasible solution from both a technical and economic way.

## **Conclusions**

This paper presents the container monitoring system developed in the IBBT MoCo (Monitoring of Containers) project. The system is capable of monitoring the container's position, its door seal and (optionally) the cargo, and to communicate that data to the wayside via a wireless data network without incurring high operational costs. A high-level system architecture has been presented, followed by a detailed description of the communication technologies and the radio state power modes. Three different power modes (REST, Secured TransPort (STP), and Secured VEssel (SVE)) were introduced and they will be used throughout the container handling to ensure an increased energy efficiency of the battery powered MoCo devices installed on the containers.

To put a viable monitoring system in the market, it will be of key importance to balance the operational costs and service revenues. The mobile roaming costs of communication, the power consumption costs of the MoCo devices and the costs related to operating the management platform are the most critical operational costs. The mobile roaming is a very important cost factor that has to be in balance with the service revenues. Since the data traffic is limited and service bundles of at least 1 MB are offered, it is difficult to further optimize the system to lower these data traffic costs. The power consumption (and the related battery replacement process) on the other hand is a very critical factor, and an optimization of the system is of high importance. By introducing the different power modes and optimizing the design parameters, the battery



lifetime can be increased to three years or more, which makes the MoCo solution a very robust monitoring system.

## **Acknowledgements**

The IBBT MoCo project is cofunded by IBBT (Interdisciplinary institute for Broadband Technology) a research institute founded by the Flemish Government. Companies and organizations involved in the project are Multicap and Rmoni, with project support of IWT (Agency for Innovation by Science and Technology in Flanders). A special thanks to Staf Van den Bulck and Jan Van Herbruggen from Multicap for their valuable input.

## **References**

- [1] Mahlknecht, S. and Madani, S.A., “On Architecture of Low Power Wireless Sensor Networks for Container Tracking and Monitoring Applications”, *Industrial Informatics, 2007 5th IEEE International Conference on*, 23-27 June 2007, pp.353-358.
- [2] Schaefer, S., “Secure trade lane: a sensor network solution for more predictable and more secure container shipments”, In *Companion To the 21st ACM SIGPLAN Symposium on Object-Oriented Programming Systems, Languages, and Applications*, Portland, Oregon, USA, October 22 - 26, 2006, pp. 839-845.
- [3] Lauf, J. O. and Gollmann D., “Monitoring and security of container transport”, In *Proceedings of New Technologies, Mobility and Security*, 2007.
- [4] Rogoz, D., O'Reilly, F., and Delaney, K., “Multi-hopping and Ad hoc Networking for Tracking Systems”, *WiSen 2007, 2nd Workshop on Wireless Sensor Networks Research in Ireland*, June 12, 2007.

- [5] Rogoz, D., O'Reilly, F., and Delaney, K., "Dedicated Networking Solutions for a Container Tracking System", In: *Ambient Intelligence with Microsystems, Microsystems*, Volume 18, 2009, pp. 387-408.
- [6] Jedermann, R., Behrens, C., Laur, R., Lang, W., "Intelligent containers and sensor networks, Approaches to apply autonomous cooperation on systems with limited resources", In: Hülsmann, M.; Windt, K. (eds.): *Understanding Autonomous Cooperation & Control in Logistics – The Impact on Management, Information and Communication and Material Flow*. Springer, Berlin, 2007, pp. 365-392.
- [7] Lang, W., Jedermann, R., Mrugala, D., Jabbari, A., Krieg-Brückner, B., and Schill, K., "The "Intelligent Container"—A Cognitive Sensor Network for Transport Management", *Sensors Journal, IEEE* , vol.11, no.3, March 2011, pp.688-698.
- [8] Su Jin Kim, Guofeng Deng, Gupta, S.K.S., and Murphy-Hoye, M., "Intelligent networked containers for enhancing global supply chain security and enabling new commercial value", *Communication Systems Software and Middleware and Workshops*, 2008. *COMSWARE 2008. 3rd International Conference on*, 6-10 Jan. 2008, pp.662-669.
- [9] Su Jin Kim, Guofeng Deng, Gupta, S.K.S., and Murphy-Hoye, M., "Enhancing Cargo Container Security during Transportation: A Mesh Networking Based Approach", *Technologies for Homeland Security, 2008 IEEE Conference on*, 12-13 May 2008, pp.90-95.
- [10] Yeoh, C.M., Chai, B.L., Kwon, T.H., Yi, K.O., Kim, T.H., Lee, C.S., Kwark, G.H., Lim, H., "Ubiquitous Containerized Cargo Monitoring System Development based on Wireless Sensor Network Technology", *International Journal of Computers Communications & Control*, vol. 6, no. 4, 2011, pp. 782-796.